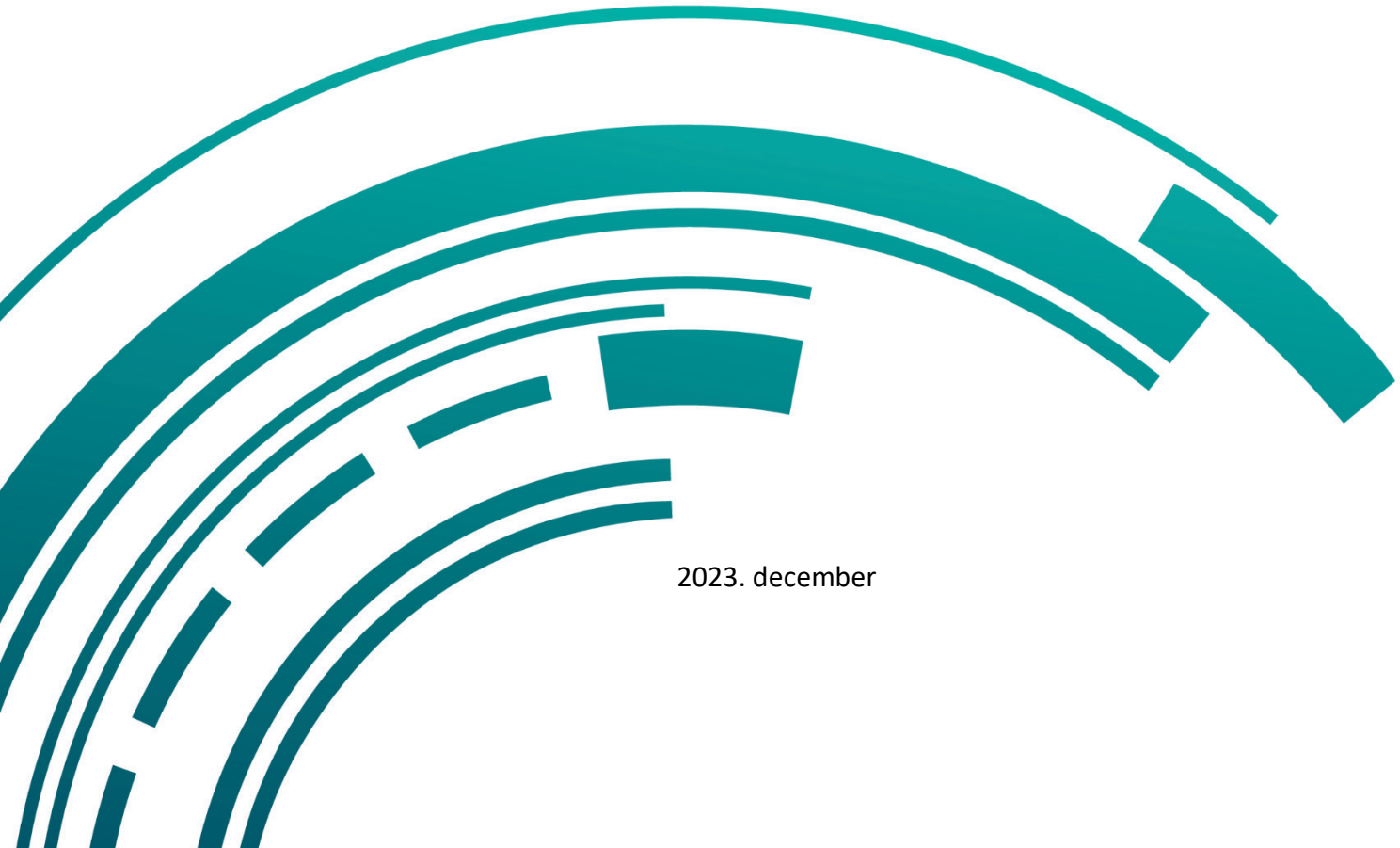
CHS Esettanulmány

GRC ÚT, AKÁR A NIS2 MEGFELELÉSHEZ



2023. december

„Amikor tényleg baj van”

Mint a hírekből ismert, a magyar IT disztribútori piac egyik legnagyobb szereplője, a CHS Hungary Kft. 2023 februárjában egy zsarolóvírusos támadást szenvedett el. Ugyan adatvesztés nélkül, három munkanapon belül sikerült helyreállítani a működésüket az EURO ONE és további szereplők segítségével, de a támadás rávilágított több hiányosságra. A CHS a támadást követően elhatározta, hogy az EURO ONE közreműködésével fejleszteni fogja az információbiztonságát, hogy a korábbi támadáshoz hasonló szituációk ne ismétlődhessenek meg.

A Kibertantv. hatálya alá eső szervezeteknek hasonló utat kell bejárniuk a megfelelőségre való felkészülés során, mint amit a CHS tett meg az elmúlt időszakban. Ezt kívánjuk ismertetni az esettanulmányunkban.

EURO ONE projektek

A CHS-t ért kiberbiztonsági incidens következtében több helyreállítási és megelőzési intézkedés megkezdésére volt szükség.

Az IT üzemeltetés támogatását az EURO ONE Adatközponti Megoldások üzletága kezdte meg , míg az InfoSec üzletág a biztonsági felkészítésben támogatja a CHS-t hálózatbiztonsági technológiák bevezetésével és üzemeltetésével, valamint a különböző felmérések végrehajtásával és a szabályozás kialakításával. A vállalatcsoportba tartozó SOCWISE Kft. pedig SOCaaS Light menedzselt szolgáltatást biztosít az információbiztonsági eseményekhez kapcsolódó jelentések készítésében és megosztásában.

Az általános Governance Risk Compliance (GRC) tanácsadói feladatok tekintetében szabad kezet kaptunk a feladatok megtervezése során. Célszerű a GRC területhez kapcsolódó felmérésekkel kezdeni a projekteket, mert ez átfogó részletinformációkat tud adni a többi projekthez. A fő cél az volt, hogy felmérjük a CHS kiinduló állapotát és megteremtsük a biztonság és ellenállóképesség GRC-hoz tartozó alapjait. A projekt hatókörébe tartozó feladatokról elmondhatjuk, hogy egy teljeskörű felmérést, üzletmenet-folytonossági tervezést és szabályozást hajtottunk végre, amit minden CHS-hez hasonló 100-200 fős, átlagos középvállalati szintű szervezetnél meg kellene valósítani:

- Üzleti hatáselemzés végrehajtása
  - *Célja*: Leállásuk esetén súlyos hatásokkal járó kritikus üzleti folyamatok azonosítása, amelyek folytonosságának vagy gyors helyreállításának biztosítása érdekében üzletmenet-folytonossági terveket (BCP) kell készíteni.
- Gap elemzés végrehajtása
  - *Célja*: Kiinduló helyzet felmérése és a meghatározott követelményrendszertől történő eltérések (hiányosságok azonosítása).
- Kockázatelemzés végrehajtása
  - *Célja*: A kockázatelemzés célja az volt, hogy az előző felmérés során azonosított hiányosságokat, valamint a globális és regionális fenyegetéseket, illetve egyéb körülményeket elemezve releváns biztonsági kockázatokat azonosítsunk és azokat a módszertanunk szerint

kockázati szintekbe soroljuk. Ez alapján prioritás szerint előálltak a részletes fejlesztési javaslataink is.

- Üzletmenet-folytonossági tervezés (BCP, DRP)
    - *Célja*: Az üzleti hatáselemzés során azonosított kritikus folyamatokat támogató vagyonelemek kiesésére üzletmenet-folytonossági keretrendszert, illetve üzletmenet-folytonossági terveket (BCP) és katasztrófa elhárítási tervet (DRP) készítettünk. Ezeknek köszönhetően a 2023 februárihoz hasonló, jövőben potenciálisan bekövetkező krízishelyzeteket még felkészültebben tudja kezelni a szervezet, de ne legyen rájuk szükség!
- Információbiztonsági Szabályzat (IBSz) kidolgozása
    - *Célja*: Az IBSz-ben a kockázatelemzés során feltárt hiányosságokat is figyelembe véve dolgoztuk ki a CHS által elvárt viselkedési szabályokat és a biztonságos működés további követelményeit. Ezeket kikényszerítve és betartva a szervezet biztonságosabban tud működni és ellenállóbb lesz a támadásokkal szemben.

Tapasztalatok

Szakmai szempontból érdemes megemlíteni, hogy a CHS-nél is, mint minden más felmérés esetében, a tervezésnél figyelembe kellett venni a feladatok egymásra való épülését és emiatt a függőségeiket is. A felméréseknél fontos, hogy a megalapozott, megismételhető és összehasonlítható eredmények érdekében módszertanok alapján kell azokat végrehajtani. Az EURO ONE-nál ezekkel már rendelkeztünk a projekt előtt. Azonos, vagy egy családba tartozó szabványokat konzisztensen használtunk a felmérések és a szabályozás kialakítása során.

A GRC feladatok végrehajtása félévet vett igénybe, folyamatos közös munkával, szoros kapcsolattartással. A többi EURO ONE projekttel való összehangolás komplex projektmenedzsment megközelítést és holisztikus szemléletet igényelt. Ami GRC oldalon kockázatként vagy információkérésként jelentkezett, az egy másik csapatnál vagy üzletágnál megoldandó feladat vagy megválaszolandó kérdés. Az EURO ONE-nak nagy előnye, hogy egy szervezetként biztosít megoldásokat a projekt során felmerülő üzemeltetési és biztonsági kihívásokra.

Következmények

A zsarolóvírus támadás ez esetben nem járt adatvesztéssel, de egy következő támadás alkalmával akár súlyosabb károkat is elszenvedhet a vállalat. Ezt elkerülendő, szükség van a rendszerek és folyamatok feltérképezésére és ezek alapján biztonsági intézkedések és rendszerek bevezetésére.

Az incidens következtében a CHS olyan tudatos intézkedéseket kezdett bevezetni, amelyek előnyökkel járnak számukra. Ez sok vállalat esetében csak akkor derül ki, amikor már megtörténik a probléma. Megfelelő biztonságtudatosság esetén ezeket az intézkedéseket a cégek megelőző jelleggel teszik meg, így egy esetleges támadást felkészülten, kevesebb kockázattal tudnak kezelni.

Előnyök:

- Tisztában vannak a kockázataikkal: mi az, ami veszélyezteti a folyamatos, biztonságos működést; milyen veszélyekkel, veszteségekkel jár, ha ez bekövetkezik.
- Szakértelmünkkel olyan tényezőkre is rávilágítottunk, amire a vállalat tapasztalat, megfelelő szaktudás hiányában nem gondolt.
- Az elkészített riportnak és tanácsadásnak köszönhetően felül tudják vizsgálni a működésüket a jövőben és el tudják kezdeni megoldani a feltárt problémáikat.

NIS2

Az előző fejezetekben felsorolt feladatok végrehajtása szükséges lesz a NIS2 irányelv és a Kibertantv. hatálya alá tartozó szervezeteknek is. A Kibertantv. által előírt elektronikus információs rendszerek és azok fizikai környezetének a biztonságának megteremtése során a védelemnek ki kell terjednie az alábbiakra:

- az információbiztonsági irányítás rendszerére,
- az elektronikus információs rendszerek kockázatainak feltárására és kezelésére,
- a kockázatok csökkentésére irányuló, a szervezet kockázatelemzésében rendszerenként meghatározandó biztonsági osztálynak megfelelő adminisztratív, logikai és fizikai intézkedések alkalmazására,
- a biztonsági események megelőzésére, felismerésére, kezelésére és hatásainak csökkentésére,
- az üzletmenet folytonosság biztosítására és
- az elektronikus információs rendszerek és az ezek által használt szoftver és hardver termékek beszerzésére, fejlesztésére, és üzemeltetésére.

A megfelelésre való felkészítés és az ezt megalapozó felmérések során a CHS GRC projektben alkalmazott alapfeladatokat és megközelítés alkalmazását javasoljuk az érintett szervezetek részére.